RECEIVED
CENTRAL FAX CENTER

NOV 0 8 2005

Appl. No. 09/275,514 Attorney Docket: 042390.P7034

In The United States Patent and Trademark Office
Before The Board of Patent Appeals and Interferences

In re Patent Application of:	Holliman, *et al.*	Examiner:	Vig, Naresh
		Art Unit:	9862
Application No.:	09/275,514		
Filed:	March 24, 1999		
For:	PARTIAL PROTECTION OF CONTENT		

APPEAL BRIEF
IN SUPPORT OF APPELLANTS' APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Honorable Director of the United States Patent and Trademark Office
Washington, DC 20231

Sir/Madam:

Applicants (hereafter "Appellants") hereby submit this Brief in support of their Appeal from a final decision by the Examiner in the above-captioned case. Appellants respectfully request consideration of this Appeal by the Board of Patent Appeals and Interferences for allowance of the claims in the above-captioned patent application.

An oral hearing is not desired.

11/10/2005 MBINAS 00000028 500221 09275514
02 FC:1402 500.00 DA

PAGE 6/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

TABLE OF CONTENTS

PAGE 7/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

1. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

2. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, of have a bearing on the Board's decision.

3. STATUS OF THE CLAIMS

Claims 1-32 are now pending in the above referenced patent application. Claims 1-32 were rejected in the Final Office Action mailed on April 06, 2005 and are the subject of this appeal.

4. STATUS OF THE AMENDMENTS

No amendments have been filed subject to the Final Rejection.

A copy of all claims on appeal is attached hereto as Appendix A.

PAGE 8/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

5. SUMMARY OF THE CLAIMED SUBJECT MATTER

With the advent of digital media and the increasingly widespread use of the Internet, cable, and satellite transmissions, the amount of content creation is dramatically increasing. Examples of content include video images and still images, with or without audio, and audio alone. Content may be created for commercial purposes such as entertainment and advertising, or for more personal interests such as home movies and information for the hobbyist. Examples of entertainment include movies which are available on DVD (digital video disks) in one of the MPEG (moving picture expert group) formats. (U.S. Publication 2002/0188570 A1, paragraph 4).

The invention concerns partially protecting content to be provided to remote computers, only some of which will have the ability and permission to undo the partial protection and produce the entire content remotely. There are a variety of reasons to partial protect content and allow restricted undoing of the protection. For example, under one use, the invention includes placing vacation videos on the World Wide Web, but protecting some segments, such as those showing children. Then, certain family members or friends can see all segments, while other members of the public can see only the undo protection of segments.

Another use includes placing an entire movie on a disc (such as a DVD) but protecting certain segments of the movie. Access to these segments would be available with the correct key including a password. Under one scenario, the protected segments include subject matter which some parents might not want their young children to view. The password could be included on a piece of paper included with the disc. Persons knowing the password could watch the entire movie, while others would watch only the undo protection of segments. Under another scheme, clips (teasers) for the movie could be undo protection of segments, while the movie itself would

PAGE 9/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

be protected. A user could obtain the password for a fee. There may be two levels of passwords. One level allows the person to see the entire video and another allows to see only certain scenes. (U.S. Publication 2002/0188570 A1, paragraphs 32 & 33).

Referring to FIG. 1, a content providing system 14 provides partially protected content through a link 18 to multiple receiving computers, of which remote receiving computers 20, 22, and 24 are examples. Displays 48, 50, and 52 may be physically integrated with or separate from remote receiving computers 20, 22, and 24. Link 18 represents any of various links including the Internet, an intranet, a local area network, a satellite network, or other networks. (As described below, the partially protected content may also be transferred on a machine readable medium such as a disc.) Examples of protection include visual scrambling and bit encryption. Content providing system 14 includes a computer or computers. As used herein, the term computer is intended to be broadly interpreted to include a variety of systems and devices including personal computers, mainframe computers, set top boxes, digital versatile disc (DVD) players, and the like. Content providing system 14 includes content 30 which may be stored in system 14 in various forms. Examples of content include video images, still images, and graphics, each with or without audio. The video is not restricted to any particular format. It may be one of the MPEG formats.

In the specific illustrated example, content 30 includes a group of segments (which may be called shots in the case of video). For example, FIG. 2 illustrates exemplary segments 1 - 7, each having a different number of frames. The seven segments form a group. The segments may be sequential segments created from a previously continuous source (such as a continuous video signal) or from previously disconnected sources (such as joining together previously disjointed video shots).

PAGE 10/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

Referring to FIGS. 1 - 3, a user interface 32 and authoring mechanism 34 are used to select at least one (a set) of the segments of content 30 to be protected. Authoring refers to selecting a segment for protection. User interface 32 may include a keyboard, mouse, and a graphical user interface (GUI) on a display. The GUI may be represented in a variety of forms and include a variety of information. For example, referring to FIG. 3, a GUI presented on a display 60 includes the following information and options, but not all these are required and other information and options could be included. Display 60 includes a window 64 that displays images from the segments in displays 66, 68, 70, 72, and 74. The images displayed may be the first frame of each segment. For example, image I1 represents the first frame of segment 1, image I2 represents the first frame of segment 2, etc. of FIG. 2. In display 64, only five of the segments of the group are displayed at a time. A scroll bar 78 can be used to select which five of the segments are represented in displays 66 - 74. For example, as the scroll bar moves to the right, the image I5 may be moved to where I4 was, and image I4 may move to where image I3 was, etc., and an image for the first frame of segment 6 appears where image I5 was. The symbol "L" below displays 66 – 74 represents the length of each displayed segment. The length of the segments may be measured in time duration and/or number of frames. Also the length (in time duration and/or number of frames) from the first frame of the first slot may be calculated.

A window 80 includes a display 84 for displaying one of the segments, which may be selected, paused or stopped through icons 90 or other means. A scroll bar 82 may be used to advance through frames of the segment selected for viewing in display 84. The various icons described herein can be activated through a mouse. Activation of a browse icon 92 may cause segment in display 66 to also appear in display 84. Bit encryption and visual scrambling selection boxes 94 and 96 can be checked with a click of a mouse to select bit encryption and/or

PAGE 11/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

visual scrambling features described below. In some embodiments, when either of these boxes is checked, the corresponding display in window 64 is enclosed in a rectangle or otherwise designated as being protected. The protection occurs in response to encode icon 98 being activated with a click of a mouse. For example, display 68 and 74 are enclosed in a rectangle indicating that segments 2 and 5 (which include images I2 and I5) will be protected if encode icon 98 is activated.

There are at least two ways in which a RCN (e.g., a PN) may be used. In some embodiments, the RCN is used as a component of a key. In other embodiments, the RCN is in a table stored in the scrambling computer and is matched against the remote RCN during playback. This second way may be useful where the content is target to multiple users.

In the above described system, the default condition is to not protect segments and the user has to do something (e.g., check box 94 and/or 96) to select them for protection. In essence, the other segments are selected to be not protected by the failure to select them to be protected. Under an alternative system, the default condition may be to protect segments and the user has to do something to select them to not be protect. Under still another system, a user may have to designate whether a segment is to be protected or not protected.

In some embodiments, a remote computer number (RCN) is used as part of a key to protect the segments (e.g., with bit encrypting and/or visual scrambling). The remote computer number is number associated with a remote computer and is used to undo the protection remotely. Examples of remote computer number include a processor number (PN) associated with a particular processor, a chipset number associated with a particular chipset, and a software number that is associated with particular software, such as an operating system, or a combination of them. In the example of FIG. 3, the remote computer number is a processor number (PN) 102

PAGE 12/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

displayed between the parenthesis. If this PN feature is included in the key, the remote receiving computer will need a processor having a processor number that matches the processor number selected. Otherwise, decoding will not occur and the protected segments will remain protected.

Password box 104, Input File box 106, and Output File box 108 allow typing of passwords, and designations for the input and output files of the segments. Other means may be used for providing the password and input and output files. A password is used for encoding (bit encryption and/or visual scrambling) the segments selected for protection. The same password is used in the remote receiving computer to undo the protection of the protected segment.

FIG. 4 illustrates a content providing system 114 which is similar to content providing system 14 but illustrates some additional capabilities, which could be included in content providing system 14. A segment creation mechanism 120 represents a user interface and associated software to select segments of the group of segments (e.g., to designate the beginning and ending frames or time of the segment). Mechanism 102 may be used for joining disjointed segments in a group and/or dividing continuous content into segments of a group.

The remote computer number (RCN) mechanism 124 represents software to obtain a remote computer number of the remote receiving computer (e.g., computer 20). The remote computer number can be obtained in various ways (e.g., through a secure socket layer applet sent to the remote receiving computer). The user of the remote receiving computer could request software that is downloaded from content providing system 114. Upon receiving the correct password, the software interfaces with content providing system 114 to obtain the remote computer number of the remote receiving computer, which may be stored in a RCN database 126 so the remote computer number does not have to be obtained again. Passwords may also be stored. Protected content may be stored in stored content memory 128. There may be different

PAGE 13/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

stored contents for different combinations of remote computer numbers and passwords. As noted, the invention does not require a remote computer number. The various mechanisms described herein may be implemented in hardware or through software or firmware run on a processor 132.

Referring to FIG. 5, the invention is not limited to use with a physical link. Rather, the group of segments may be written by a disc writer 136 onto a disc 138. Which is inserted into a disc drive 142 of a remote receiving computer 140. Assuming remote receiving computer 140 has the correct key, media player 144 undoes the protection of the set of segments, and the entire group of segments may be displayed on display 146. (U.S. Publication 2002/0188570 A1, paragraphs 35 & 46).

PAGE 14/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The above referenced patent application has been reviewed in light of the Office Action, dated April 06, 2005, in which:

- claims 1-16, and 19-32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis *et al.* (hereafter, 'Lewis,' US Patent No. 6,385,388 B1) in combination with Hsu (US Patent No. 6,195,692 B1) in further combination with DirecTV;
- and claims 17 and 18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in combination with Hsu and DirecTV in further combination with DirecTV in further combination with "Ratings, Filters, and Censorship" by Gary Robson (hereafter, 'Robson').

PAGE 15/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

7. ARGUMENT

7.1. 35 U.S.C. § 103(a)

7.1.1. Lewis, Hsu, and DirecTV: Claims 1-16, and 19-32

The PTO has also rejected claims 1-16, and 19-32 under 35 U.S.C. § 103(a) based upon Lewis and Hsu in combination with DirecTV. The rejection of these claims is respectfully traversed.

7.1.1.1 Official Notice

It is noted that the April 2005 Office Action does not cite Official Notice in the summary paragraph of the rejection (page 3, paragraph 3); however, the term Official Notice occasionally appears within the detailed explanation of the rejection of various claims. For example, claims 2 & 13 on page 13, paragraph 2.

Appellants are unsure if the PTO intended to base the rejection on this Official Notice or if the Notice had been withdrawn and merely inadvertently included from previous Office Actions.

Regardless, the PTO's Official Notice of the use of "business choice" is respectfully traversed. The PTO claims "Official notice it [*sic*] taken that it would have been obvious to one of ordinary skill in the art at the time the invention was made that it is a business choice to select what part of [*sic*] data stream need [*sic*] to be scrambled to prevent unintended use of the data."

Appellants respectfully note that the PTO is not taking Official Notice of a technology or bit of scientific knowledge, but instead the PTO is taking Official Notice of what one skilled in the art would consider obvious. In other words, the PTO is attempting to establish a *prima facie*

PAGE 16/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

case of obviousness by taking Official Notice of the legal conclusion of obviousness. M.P.E.P. § 2144.03, which deals with Official Notice, is entitled "Reliance on Common Knowledge in the Art or 'Well Known' Prior Art," and in the first sentence clearly directs Official Notice only to findings of fact. It is respectfully asserted the Official Notice is inappropriate, because the PTO may not take Official Notice of a legal conclusion, but instead must limit itself to findings of fact regarding prior art.

Furthermore, Appellants have previously traversed a similar Official Notice and requested that the PTO provide documentary evidence supporting the Notice. Appellants respectfully assert that M.P.E.P. § 2144.03(C) requires that "the Examiner Must Support the Finding With Adequate Evidence." As far as Appellants can tell, this has not been done. Appellants note that this may be because the Notice was withdrawn but inadvertently included from a previous Office Action in the detailed discussion of the claim rejections.

As detailed in M.P.E.P. § 2144.03, the standard of review applied to findings of fact is the "substantial evidence" standard under the Administrative Procedure Act (APA). See *In re Gartside*, 203 F.3d 1305, 1315, 53 USPQ2d 1769, 1775 (Fed. Cir. 2000). Appellants respectfully request that the PTO furnish documentary evidence showing prior art that alone or in combination meets all the elements of the Appellants' claimed subject matter and showing why one skilled in that art would be motivated to combine the subject matter of the other cited art.

PAGE 17/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

7.1.1.2 Remarks

M.P.E.P. § 706.02(j) sets forth the standard for a § 103(a) rejection:

> To establish a prima facie case of obviousness, three basic criteria must be met.
>
> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings.
>
> Second, there must be a reasonable expectation of success.
>
> Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
>
> The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (whitespace added).

Appellants begin with claim 1. Claim 1 recites:

> 1. (Previously Presented) A method of providing content to a receiving device having an associated identifier associated with a network address for the receiving device, comprising:
> selecting a set of segments of content from a group of segments to be protected wherein the set does not include all segments of the group;
> protecting the segments of the set, but not the other segments of the group, to prevent the protected segments from being properly reproduced unless the protection is undone with assistance of a correct key that is not generally available and is based at least in part on the associated identifier: and
> providing access to the group of segments over a network.

Appellants respectfully assert that the combination set forth by the PTO fails to meet the requirement for a *prima facie* case for a § 103(a) rejection for at least the following reasons.

It is respectfully asserted that neither Lewis, Hsu, nor DirecTV, either alone or in combination, suggests or describes decrypting the segments utilizing **a correct key that is** ... **based** at least in part **on the associated identifier with a network address** for the receiving device. See, claim 1, lines 2, 7, & 8. The PTO asserts that the DirecTV teaches this limitation. However, it is respectfully asserted that DirecTV does **not** teach this limitation.

PAGE 18/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

DirecTV instead shows **an access card that must be activated prior to decrypting content**. See DirecTV, page 15, cited by the PTO and quoted, in part, below.

> **I purchased a DSS system from a friend of mine. What do I have to do to get the system installed and activate programming?**
>
> There are three steps to follow when activating a previously owned system.
>
> First, the original owner, when turning a system over to a new individual, should contact DIRECTV and/or USSB to de-activate his/her access card. This is for the original owner's protection.
>
> Second, the new owner should contact DIRECTV right away at 1-800-DIRECTV to order a new access card. DIRECTV initially charges a $150 activation fee for a new access card to be issued to the new subscriber. DIRECTV will mail the individual a pre-addressed, postage paid envelope to send back the old (original) access card. When the new subscriber mails back the original owner's access card, DIRECTV will credit the new subscriber $115 for returning the card. Hence, the new subscriber is only charged $35 for the new card. If the new owner chooses not to mail back the old access card, he/she will be charged the full $150. The process of switching out access cards protects the new subscriber from any prior charges incurred by the previous owner, and identifies the new owner as a new DIRECTV subscriber.
>
> Third, once the new owner receives an access card, he/she can call DIRECTV to immediately activate service. The individual should state to the DIRECTV representative that he/she has purchased a pre-owned DSS receiver and would like to activate programming at his/her new address.

Appellants respectfully assert that any mention of "address" in the quote above refers to a physical street address not a network address.

Appellants admit that at a cursory level this resembles portions of claim 1, but it does not actually met the § 103 requirement to "teach or suggest all the claim limitations." Specifically, DirecTV does not teach a **key that is based** at least in part **on the associated identifier with a network address**. The DirecTV document is silent on how the device decryption actually works. The reader (be it the PTO or the Appellants) is required to guess as to how the decryption functions.

For example, the DirecTV access card **may** decrypt signals based upon:

PAGE 19/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

1. a key, universal to all DirecTV access cards, that is transmitted from the satellite to the card;
2. a key, universal to all DirecTV access cards, that is transmitted to the card via the DirecTV telephone line via activation; or
3. a key, universal to all DirecTV access cards, that is embedded within the access card but not activated until a control signal is received from the satellite.

Appellants point out that all of these suggestions as to how the DirecTV reference fulfills the decryption function are guesses, because the DirecTV document is silent on how the decryption is done. These guesses are just as valid as the PTO's guess that the DirecTV system decodes signals based upon an identifier, associated with the access card (as opposed to a universal key).

It is unlikely that DirecTV encodes their broadcast in such a way that there is a key associated with either a network address or an identifier on each card. DirecTV issues a single broadcast to all or half the United States (Appellants are unsure if DirecTV has both an East and a West Coast satellite). These satellites have a limited bandwidth with which to transmit the TV broadcasts.

If the PTO's guess as to how DirecTV worked was correct, each receiver would have an individual network address (supposedly embedded within the access card). Each receiver would receive a broadcast specially encrypted with that receiver's unique key (which is required to be based upon the receiver's network address). Therefore, the satellite must broadcast not 1 channel of HBO to everyone in the US but instead 1 channel of HBO encrypted for receiver #1, and another channel of HBO encrypted for receiver #2, yet another channel of HBO encrypted for

PAGE 20/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

receiver #3, and so on for each receiver in the US. DirecTV would be required to use their limited bandwidth for millions of channels (assuming there are millions of DirecTV subscribers), all identical in content except for the encryption. Appellants respectfully assert that it is not probable that DirecTV works in this fashion; however, this is how DirecTV would be required to work if, as the PTO contends, the key was based upon the receiver's "network address" as opposed to a universal key.

It is respectfully asserted that the Code (35 U.S.C. § 103) does not allow prior art that may with hindsight possibly within some variation produce a limitation included within the claims. Instead, the Code specifies that the cited art must **explicitly** teach or suggest the limitation. It is respectfully asserted that all the DirecTV teaches is an access card, not a "**correct key that is** not generally available and is **based at least in part on the associated identifier**" with a network address. See, claim 1, lines 2, 7, & 8.

Under the requirements for §103, the prior art reference (or references when combined) must teach or suggest all the claim limitations. It is respectfully asserted that neither Lewis, Hsu, nor DirecTV, either alone or in combination, suggests or describes a receiving device having "**correct key that is** not generally available and is **based at least in part on the associated identifier**."

Therefore, even if the combination were proper, although Appellants believe that it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claims. It is, therefore, respectfully requested that the rejection of this claim be withdrawn.

PAGE 21/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

7.1.1.3 Remaining Claims

Claims 2-16, and 19-32 either depend from and include the limitations of claim 1, or include a substantially similar and patentably distinct limitation as claim 1. Therefore, these claims patentably distinguish from the cited patents on the same basis as claim 1. It is, therefore, respectfully requested that the PTO withdraw the rejections of these claims.

PAGE 22/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

7.1.2. Lewis, Hsu, DirecTV, & Robson: Claims 17 and 18

7.1.2.1 Remarks

The PTO has also rejected claims 17 and 18 under 35 U.S.C. § 103(a) on Lewis, Hsu, DirecTV and in combination with Robson. The rejection of these claims is also traversed.

Appellants begin with claim 17. Claim 17 recites:

> 17. (Original) The method of claim 12, wherein information identifying protected segments is contained in at least one watermark.

Claim 17 ultimately depends from the independent claim 12. Claim 12 recites:

> 12. (Previously Presented) A method of receiving and processing content by at least one receiving device having an associated identifier with a network address for the receiving device, comprising:
>
> accessing over a network a group of segments of content including a set of segments that does not include all segments of the group, and wherein the set, but not the other segments of the group, have been protected to prevent the protected segments from being properly reproduced without undoing the protection with assistance of a correct key that is not generally available and is based at least in part on the associated identifier;
>
> undoing the protection if the correct key is received; and
>
> playing the group of segments seamlessly with a media player.

Appellants respectfully assert that the combination set forth by the PTO fails to meet the requirement for a *prima facie* case for a § 103(a) rejection for at least the following reasons.

It is respectfully asserted that neither Lewis, Hsu, DirecTV, nor the Robson, either alone or in combination, suggests or describes **a correct key that is** ... **based at least in part on the associated identifier with a network address**.

As described in detail above, the PTO asserts that the DirecTV teaches this limitation. However, it is respectfully asserted that DirecTV does **not** teach this limitation. DirecTV instead shows **an access card that must be activated prior to decrypting content**. See DirecTV, page

PAGE 23/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

15, paragraph 9. The DirecTV document is silent on how the device decryption actually works. The reader (be it the PTO or the Appellants) is required to guess as to how the decryption functions. Because the Code specifies that the cited art must explicitly teach or suggest the limitation, DirecTV does not meet the standard set for establishing a *prima facie* case of obviousness.

Therefore, even if the combination were proper, although Appellants believe that it is not, nonetheless, the combination would still fail to produce the invention as recited in the rejected claims. It is, therefore, respectfully requested that the rejection of this claim be withdrawn.

Claim 18 either depend from and include the limitations of claims 17 or 12, or include a substantially similar and patentably distinct limitation as claim 17 or 12. Therefore, these claims patentably distinguish from the cited patents on the same basis as claim 17 or 12. It is, therefore, respectfully requested that the PTO withdraw the rejections of these claims.

PAGE 24/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

8. CONCLUSION

In view of the foregoing, it is respectfully asserted that all claims pending in this application, as amended, are in condition for allowance. If the Examiner has any questions, they are invited to contact the undersigned at 503-264-7002. Reconsideration of this patent application and early allowance of all claims is respectfully requested.

Respectfully submitted,

Dated: Tue Nov 8, 2005

Justin B. Scout
Reg. No. 54,431

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd., Seventh Floor
Los Angeles, CA 90025-1026
(503) 264-0967

PAGE 25/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

APPENDIX A: CLAIMS ON APPEAL

1. (Previously Presented) A method of providing content to a receiving device having an associated identifier associated with a network address for the receiving device, comprising:

selecting a set of segments of content from a group of segments to be protected wherein the set does not include all segments of the group;

protecting the segments of the set, but not the other segments of the group, to prevent the protected segments from being properly reproduced unless the protection is undone with assistance of a correct key that is not generally available and is based at least in part on the associated identifier: and

providing access to the group of segments over a network.

2. (Original) The method of claim 1, wherein selecting the set involves selecting at least some of the set for visual scrambling and protecting the set includes visual scrambling those segments selected for visual scrambling.

3. (Previously Presented) A method of providing content, comprising:

selecting a set of segments of content from a group of segments to be protected wherein the set does not include all segments of the group:

protecting the segments of the set, but not the other segments of the group, to prevent the protected segments from being properly reproduced unless the protection is undone with assistance of a correct key that is not generally available:

providing access to the group of segments over a network:

PAGE 26/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

wherein selecting the set involves selecting at least some of the set for visual scrambling and protecting the set includes visual scrambling those segments selected for visual scrambling; and

wherein visual scrambling involves using a key, including a remote computer number.

4. (Original) The method of claim 3, wherein the remote computer number is a processor number.

5. (Original) The method of claim 2, wherein selecting the set involves designating those segments to be protected.

6. (Original) The method of claim 1, wherein selecting the set involves selecting at least some of the set for bit encryption and protecting the set includes bit encrypting those segments selected for bit encryption.

7. (Original) The method of claim 1, wherein selecting the set involves selecting at least some of the set for visual scrambling and at least some of the set for bit encryption, wherein some of the set may be selected for both visual scrambling and bit encryption, and protecting the set includes visual scrambling those segments selected for visual scrambling and bit encrypting those segments selected for bit encryption.

8. (Original) The method of claim 1, wherein a remote computer number is stored and matched against a remote computer number from a remote receiving computer during playback.

PAGE 27/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

9. (Original) The method of claim 1, wherein prior to protection, the segments include video signals.

10. (Original) The method of claim 9, wherein the video signals are in an MPEG format.

11. (Original) The method of claim 1, wherein prior to protection, the segments include video and audio and both the video and audio are protected.

12. (Previously Presented) A method of receiving and processing content by at least one receiving device having an associated identifier with a network address for the receiving device, comprising:

accessing over a network a group of segments of content including a set of segments that does not include all segments of the group, and wherein the set, but not the other segments of the group, have been protected to prevent the protected segments from being properly reproduced without undoing the protection with assistance of a correct key that is not generally available and is based at least in part on the associated identifier;

undoing the protection if the correct key is received; and

playing the group of segments seamlessly with a media player.

13. (Previously Presented) The method of claim 12, wherein at least some of the protected segments have been protected through visually scrambling.

PAGE 28/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

14. (Original) The method of claim 12, wherein at least some of the protected segments have been protected through bit encryption.

15. (Original) The method of claim 12, wherein the key includes a remote computer number.

16. (Original) The method of claim 12, wherein information identifying protected segments is contained in headers.

17. (Original) The method of claim 12, wherein information identifying protected segments is contained in at least one watermark.

18. (Original) The method of claim 12, wherein information identifying protected segments is contained in data transmitted separately from the segments.

19. (Previously Presented) A content providing system, comprising:

storage to hold at least content divided into segments and an identifier associated with a network address for a receiving device:

a user interface; and

circuitry and software cooperating with the user interface to select a set of the segments to be protected from a group of segments, wherein the set does not include all segments of the group, and to protect the set of segments, but not the other segments of the group, to allow access to the unprotected segments over a network but to prevent the protected segments from being properly reproduced over the network unless the protection is undone with assistance of a correct

PAGE 29/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

key that is not generally available, wherein the correct key is based at least in part on the associated identifier.

20. (Original) The content providing system of claim 19, wherein protecting the selected segments involves a key including a remote computer number.

21. (Original) The content providing system of claim 19, wherein the user interface includes options to select at least some of the set of segments to be visually scrambling and the protecting of the segments selected for visual scrambling includes visual scrambling.

22. (Original) The content providing system of claim 19, wherein the user interface includes options to select at least some of the set of segments to be bit encrypted and protecting of the segments selected for bit encryption includes bit encryption.

23. (Original) The content providing system of claim 19, wherein the user interface includes options to select at least some of the set of segments to be visually scrambled and at least some of the set of segments to be bit encrypted, wherein some of the set of segments may be selected for both visual scrambling and bit encryption, and protecting of the segments selected for visual scrambling includes visual scrambling and protecting of the segments selected for bit encryption includes bit encryption.

24. (Original) The content providing system of claim 19, wherein the content includes video signals.

PAGE 30/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

25. (Original) The content providing system of claim 19, wherein the content includes video signals and audio signals.

26. (Previously Presented) An article comprising:

a machine readable media including instructions that when executed cause a content providing system to:

select a set of segments of content from a group of segments to be protected wherein the set does not include all segments of the group;

protect the segments of the set with, but not the other segments of the group, to prevent the protected segments from being properly reproduced unless the protection is undone with assistance of a correct key that is not generally available, wherein the correct key is based at least in part on an identifier associated with a network address for a receiving device; and

provide access to the group of segments over a network.

27. (Original) The article of claim 26, wherein protecting the selected segments involves a key including a remote computer number.

28. (Previously Presented) An article comprising:

a machine readable media including instructions that when executed cause a content providing system to:

access over a network a group of segments of content including a set of segments that does not include all segments of the group, and wherein the set, but not the other segments of the

PAGE 31/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

group, have been protected to prevent the protected segments from being properly reproduced without undoing the protection with assistance of a correct key that is not generally available, wherein the correct key is based at least in part on an identifier associated with a network address for a receiving device for the content;

undo the protection if the correct key is received; and

play the group of segments seamlessly with a media player.

29. (Original) The article of claim 28, wherein the key includes a remote computer number.

30. (Previously Presented) A method of providing content to at least one receiving device having an associated identifier associated with a network address for a receiving device, comprising:

selecting a set of segments of content from a group of segments to be protected wherein the set does not include all segments of the group;

protecting the segments of the set, but not the other segments, through visual scrambling determined based at least in part on the associated identifier; and

providing access to the group of segments over a network.

31. (Previously Presented) The method of claim 30, wherein the receiving device comprises a network information browser configured to display the provided content.

PAGE 32/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22

32. (Previously Presented) The method of claim 15, wherein the remote computer number is the associated identifier.

PAGE 33/33 * RCVD AT 11/8/2005 8:51:26 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID: * DURATION (mm-ss):11-22